

BÁO CÁO
Tình hình an ninh mạng tháng 9 năm 2026

Thực hiện chức năng, nhiệm vụ đơn vị chuyên trách về an ninh mạng, Công an tỉnh báo cáo kết quả giám sát an ninh mạng đối với các hệ thống thông tin quan trọng dùng chung, hệ thống mạng nội bộ (LAN) và mạng Truyền số liệu chuyên dùng cấp II của tỉnh Hưng Yên như sau:

I. TÌNH HÌNH

1. Tình hình liên quan hoạt động tấn công mạng tại Việt Nam

- Từ ngày 16/8/2026 đến ngày 15/9/2026, NCA đã phân tích, tổng hợp các sự kiện an ninh mạng đáng chú ý tại Việt Nam, gồm: hoạt động tấn công mạng của nhóm tin tặc Mustang Panda; hoạt động tấn công mạng nhằm vào doanh nghiệp trong nước; hoạt động tấn công mạng nhằm vào hệ thống thông tin cơ quan nhà nước và tác nhân đe dọa mới “Nie” sử dụng trí tuệ nhân tạo (AI) thực hiện các chiến dịch xâm nhập mạng tại khu vực châu Á.

1.1. Hoạt động tấn công mạng của nhóm tin tặc Mustang Panda

- Qua công tác phối hợp, rà soát mã độc với các đơn vị, NCA thu thập được biến thể mã độc của nhóm tin tặc Mustang Panda được sử dụng để tấn công vào hệ thống thông tin ở Việt Nam. Bộ mẫu tấn công gồm 03 tệp: kmrefresh.exe (tệp sạch có chữ ký số bị lợi dụng), coreglobconfig.dll (thư viện độc hại được nạp kèm) và glob.dat (payload đã bị mã hóa).

- Phương thức tấn công: Mã độc sử dụng kỹ thuật DLL sideloading, trong đó tệp kmrefresh.exe nạp thư viện coreglobconfig.dll; hàm SyncLanguageDataToCloud() đọc và giải mã payload từ tệp glob.dat bằng phép XOR với khóa 0x19. Shellcode sau khi giải mã tiếp tục giải nén (thuật toán LZNT-1) và nạp thư viện độc hại trực tiếp trên bộ nhớ (kỹ thuật Reflective DLL); các API bị làm rối bằng kỹ thuật Stack String nhằm né tránh phần mềm phòng, chống mã độc (AV, EDR).

- Để duy trì hoạt động, mã độc sao chép các tệp vào thư mục “C:\Program Files (x86)\Common Files\System\kme” và tạo dịch vụ có tên “Kme Crash Handler”; kết nối đến máy chủ điều khiển (C2) qua các giao thức HTTP, UDP, TCP, ICMP để nhận lệnh, cho phép đối tượng liệt kê, sao chép, đổi tên, xóa, di chuyển tệp tin, tắt máy và thực thi các lệnh khác trên máy tính nạn nhân. Máy chủ điều khiển ghi nhận gồm: www.aihkstore.com (cổng 80, 443) và sports.daliylog.shop (cổng 110, 8080).

- Nhận định: Qua công tác rà soát cho thấy nhiều đơn vị vẫn còn bị nhiễm dòng mã độc của nhóm tin tặc Mustang Panda, dẫn đến nguy cơ bị chiếm quyền điều khiển, lộ, mất tài liệu, bí mật nhà nước. Hạ tầng điều khiển của mã độc

trùng khớp với hạ tầng của nhóm đã tấn công vào lĩnh vực tài chính ngân hàng tại Việt Nam từ năm 2024, cho thấy nhóm Mustang Panda vẫn đang duy trì hoạt động và có thể đã nằm vùng lâu trong hệ thống.

1.2. Hoạt động tấn công mạng nhằm vào doanh nghiệp, cơ quan, tổ chức trong nước

- Tiếp tục theo dõi dòng mã độc tinh vi được phát hiện từ tháng 7/2026 nhằm vào doanh nghiệp Việt Nam, NCA phát hiện biến thể mới của dòng mã độc này được tin tặc sử dụng để tấn công mạng nhằm vào cơ quan, tổ chức ở Việt Nam.

- Mỗi nhử là tệp shortcut giả mạo tài liệu có tên “*Thư mời_Trung tâm Hội nghị Quốc tế.pdf.lnk*”. Khi người dùng mở tệp, đoạn lệnh đã được làm rối, mã hóa base64 sẽ được giải mã và thực thi; mã độc mở một tệp PDF để đánh lừa người dùng, đồng thời giải nén tệp addfile.2fa thành hai tệp spools.exe (tệp thực thi hợp lệ của phần mềm điều khiển từ xa TeamViewer bị lợi dụng) và libgnutls-30.dll (thư viện độc hại).

- Sau khi lây nhiễm, mã độc tạo mutex giả mạo sản phẩm bảo mật (CheckpointSecurity); giải mã cấu hình bằng thuật toán AES-CBC; tự sao chép vào thư mục “%AppData%\system” và tự xóa tệp tại thư mục ban đầu; tạo tác vụ định kỳ (Task Scheduler) tên “Security Update” giả mạo Check Point Software để duy trì hoạt động; tải payload “imusama.png” từ máy chủ điều khiển, giải mã shellcode và thực thi trực tiếp trên bộ nhớ. Tên miền điều khiển ghi nhận: webhook.hotcoffeegtax.com.

- Nhận định: Đây là mã độc được thiết kế khá tinh vi với mục đích nâng cao hiệu quả phát tán và vượt qua sự kiểm tra của phần mềm diệt virus; tên tệp tin dùng để phát tán cho thấy nhiều khả năng đây là hoạt động tấn công mạng nhằm vào cơ quan, tổ chức, doanh nghiệp ở Việt Nam.

1.3. Hoạt động tấn công mạng nhằm vào hệ thống thông tin cơ quan nhà nước

- Qua công tác nắm tình hình trên không gian mạng, NCA thu thập được mẫu mã độc có sử dụng phần mềm độc hại VShell. Đây là công cụ hậu khai thác tiềm của hậu tinh vi, đang được các nhóm APT nước ngoài (như UNC5174, Earth Lamia) sử dụng rộng rãi để thay thế Cobalt Strike nhằm duy trì quyền truy cập trái phép và thu thập dữ liệu trên hệ thống mục tiêu.

- Chuỗi lây nhiễm gồm 03 giai đoạn: (1) Tệp Service.exe là trình nạp (loader) viết bằng Golang, kiểm tra môi trường ảo hóa (tự thoát nếu RAM dưới 2 GB hoặc CPU dưới 2 nhân), giải mã payload và sử dụng kỹ thuật “ngủ” có làm rối (sleep obfuscation) để né tránh cơ chế quét bộ nhớ của EDR; (2) Thư viện nạp phản chiếu (Reflective Loader DLL) nạp mã độc trực tiếp từ RAM, không ghi tệp xuống ổ cứng; (3) Mã độc VShell (tcp_windows_amd64.dll) có cấu hình mã hóa AES, kết nối đến máy chủ điều khiển 206.238.70.142:8088 để nhận lệnh từ đối tượng.

- Nhận định: Các nhóm tin tặc, gián điệp mạng nước ngoài thường xuyên thực hiện các chiến dịch tấn công mạng nhằm vào hệ thống thông tin của các bộ, ban, ngành; sau khi kiểm soát được hệ thống, chúng tiếp tục phát tán, mở rộng tấn công, kiểm soát diện rộng nhằm thu thập thông tin.

1.4. “Nie” – Tác nhân đe dọa mới sử dụng AI thực hiện các chiến dịch xâm nhập mạng tại khu vực châu Á

- Trong tháng 7 và tháng 8/2026, Hunt.io phát hiện chiến dịch tấn công mạng tinh vi do đối tượng có biệt danh “Nie” điều hành, sử dụng khung điều phối AI mang tên SecFlow, tích hợp các mô hình ngôn ngữ lớn (Claude, Qwen, DeepSeek) để tự động hóa quy trình từ trinh sát đến khai thác lỗ hổng. Chiến dịch nhằm vào 6 quốc gia châu Á; tại Việt Nam, mục tiêu là lĩnh vực công nghiệp, dịch vụ thương mại, trong đó tập trung vào các máy chủ công nghiệp tại khu vực Đà Nẵng.

- Bộ công cụ của đối tượng gồm: khung điều phối AI SecFlow; công cụ GLUTTON tạo webshell cho nhiều nền tảng (Java, .NET, Node.js), giấu dữ liệu trong tệp ảnh PNG (steganography) và làm rối mã nguồn để vượt qua các hệ thống an ninh; tích hợp giao thức ngữ cảnh mô hình (MCP) cho phép tác nhân AI trực tiếp điều khiển công cụ tấn công; mã độc điều khiển từ xa SecBox viết bằng ngôn ngữ Go để duy trì quyền kiểm soát và mở rộng xâm nhập; hạ tầng hỗ trợ thuộc họ tên miền *.niestools.com.

- Đối tượng khai thác các lỗ hổng đã biết gồm: CVE-2014-6271 (Shellshock), CVE-2020-1938 (Ghostcat), CVE-2022-22965 (Spring4Shell), CVE-2016-4437 (Apache Shiro), CVE-2021-43798 (Grafana), CVE-2024-4956 (Nexus Repository), CVE-2021-29441 (Nacos), CVE-2021-44228 (Log4j); kết hợp sử dụng thông tin xác thực bị rò rỉ.

- Nhận định: Mô hình sử dụng tác nhân AI để điều phối, tự động hóa chuỗi tấn công dự kiến sẽ trở thành xu hướng, làm tăng nhanh tốc độ và quy mô tấn công. Tuy nhiên, chiến dịch vẫn thành công chủ yếu dựa trên những điểm yếu cơ bản như dịch vụ công khai trên Internet, ứng dụng chưa vá lỗi và thông tin xác thực bị đánh cắp, đòi hỏi các cơ quan, tổ chức phải tự động hóa khả năng phát hiện, cảnh báo và vá lỗ hổng.

2. Cảnh báo lỗ hổng bảo mật nghiêm trọng

- Từ ngày 16/8/2026 đến ngày 15/9/2026, NCA đã phân tích, tổng hợp 10 lỗ hổng bảo mật nghiêm trọng, trong đó có 06 lỗ hổng mức độ rất nghiêm trọng, 04 lỗ hổng mức độ nghiêm trọng; 08 lỗ hổng đã có mã khai thác (PoC) công khai. Một số lỗ hổng đã được khai thác trong các cuộc tấn công mạng gần đây trên thế giới và có thể ảnh hưởng đến các cơ quan, tổ chức ở Việt Nam. Cụ thể như sau:

2.1. CVE-2026-69836 – Lỗ hổng thực thi mã từ xa trên Microsoft Entra ID

- Điểm CVSS 10/10, mức độ rất nghiêm trọng. Lỗ hổng do lỗi giải tuần tự dữ liệu không đáng tin cậy (Deserialization of Untrusted Data), cho phép tin tặc

gửi các gói dữ liệu độc hại qua Internet để thực thi mã từ xa. Lỗi hồng ảnh hưởng đến toàn bộ dịch vụ đám mây Microsoft Entra ID (tên gọi cũ là Azure Active Directory).

- Khuyến nghị: Microsoft đã vá lỗi trực tiếp trên hạ tầng đám mây, người dùng không cần cài đặt bản vá. Lỗi hồng đã có mã khai thác công khai.

2.2. CVE-2026-68820 – Lỗi hồng leo thang đặc quyền trong Windows Ancillary Function Driver

- Điểm CVSS 7.0/10, mức độ nghiêm trọng. Lỗi hồng do lỗi sử dụng bộ nhớ sau khi giải phóng (use-after-free) trong trình điều khiển AFD.sys, cho phép tin tặc giành quyền SYSTEM. Lỗi hồng ảnh hưởng đến tất cả các máy trạm và máy chủ Windows (Windows 10, Windows 11 và Windows Server).

- Khuyến nghị: Cài đặt bản cập nhật bảo mật mới nhất của Microsoft và bắt buộc khởi động lại máy để bản vá có hiệu lực hoàn toàn. Lỗi hồng đã có mã khai thác công khai.

2.3. CVE-2026-64600 – Lỗi hồng leo thang đặc quyền cục bộ trong hệ thống tệp XFS của Linux Kernel

- Điểm CVSS 7.8/10, mức độ nghiêm trọng. Lỗi hồng do lỗi tranh chấp trong cơ chế sao chép khi ghi (copy-on-write) đối với các tệp được liên kết lại (reflinked files), có thể dẫn đến leo thang đặc quyền. Lỗi hồng ảnh hưởng đến các phiên bản Linux kernel từ v4.11 đến trước khi áp dụng bản vá.

- Khuyến nghị: Cập nhật kernel từ nhà cung cấp và khởi động lại hệ thống; hiện không có giải pháp tạm thời bằng cấu hình đáng tin cậy. Lỗi hồng đã có mã khai thác công khai.

2.4. CVE-2026-20079 – Lỗi hồng thực thi mã từ xa trên Cisco Secure Firewall Management Center (FMC)

- Điểm CVSS 10/10, mức độ rất nghiêm trọng. Lỗi hồng trong giao diện web cho phép tin tặc vượt qua xác thực và thực thi lệnh với quyền root bằng cách gửi các yêu cầu HTTP được tạo sẵn. Lỗi hồng ảnh hưởng đến Cisco Secure FMC các phiên bản 7.0.x (tất cả), 7.1.x (tất cả), 7.2.0 - 7.2.10.2, 7.3.0 - 7.3.1.2, 7.4.0 - 7.4.3, 7.6.0 - 7.6.3, 7.7.0 - 7.7.11.

- Khuyến nghị: Nâng cấp lên phiên bản đã được Cisco sửa lỗi càng sớm càng tốt; hiện không có giải pháp tạm thời. Lỗi hồng đã có mã khai thác công khai.

2.5. CVE-2026-42533 – Lỗi hồng tràn bộ đệm Heap trong NGINX Open Source và NGINX Plus

- Điểm CVSS 9.2/10, mức độ rất nghiêm trọng. Tin tặc gửi các yêu cầu HTTP được tạo đặc biệt gây tràn bộ đệm heap, có thể thực thi mã tùy ý hoặc gây từ chối dịch vụ (DoS). Lỗi hồng ảnh hưởng đến NGINX Open Source và NGINX Plus các phiên bản từ 0.9.6 đến 1.31.2.

- Khuyến nghị: Cập nhật lên NGINX 1.30.4, 1.31.3 hoặc NGINX Plus R37 P3 (hoặc mới hơn); trường hợp chưa thể cập nhật, sử dụng các nhóm regex có tên (named captures) để giảm thiểu. Lỗi hồng đã có mã khai thác công khai.

2.6. CVE-2026-65801 – Lỗ hổng leo thang đặc quyền trong Microsoft Exchange Online

- Điểm CVSS 10/10, mức độ rất nghiêm trọng. Tin tặc lợi dụng lỗi kiểm tra đầu vào của Exchange Online để ép máy chủ gửi các lệnh truy cập trái phép tới các dịch vụ nội bộ của Microsoft. Lỗ hổng ảnh hưởng đến tất cả các phiên bản Exchange Online; không ảnh hưởng đến Microsoft Exchange Server cài đặt trên hạ tầng riêng.

- Khuyến nghị: Microsoft đã tự động triển khai bản vá trên hệ thống máy chủ, người dùng không cần cài đặt. Lỗ hổng chưa có mã khai thác công khai.

2.7. CVE-2026-14894 – Lỗ hổng thực thi mã từ xa trong plugin Super Forms của WordPress

- Điểm CVSS 9.8/10, mức độ rất nghiêm trọng. Lỗ hổng tại trình xử lý AJAX `super_submit_form` không kiểm tra phần mở rộng, loại tệp khi tải lên, cho phép tin tặc tải lên webshell PHP và thực thi mã từ xa. Lỗ hổng ảnh hưởng đến plugin Super Forms - Drag & Drop Form Builder từ phiên bản 6.3.313 trở xuống.

- Khuyến nghị: Nâng cấp plugin lên phiên bản 6.3.314 trở lên. Lỗ hổng đã có mã khai thác công khai.

2.8. CVE-2026-85046 – Lỗ hổng Type Confusion trong công cụ JavaScript và WebAssembly V8 của Google Chrome

- Điểm CVSS 8.8/10, mức độ nghiêm trọng. Tin tặc có thể lừa người dùng truy cập trang HTML được chỉnh sửa đặc biệt để thực thi mã độc mà không cần người dùng thao tác thêm. Lỗ hổng ảnh hưởng đến Google Chrome Desktop các phiên bản trước 152.0.7977.82.

- Khuyến nghị: Nâng cấp Chrome lên phiên bản an toàn và khởi động lại trình duyệt để bản vá có hiệu lực. Lỗ hổng đã có mã khai thác công khai.

2.9. CVE-2026-47870 – Lỗ hổng Directory Traversal trong VMware Avi Load Balancer

- Điểm CVSS 8.8/10, mức độ nghiêm trọng. Lỗ hổng do giới hạn đường dẫn không đúng cách, cho phép tin tặc truy cập các vị trí tùy ý trên thiết bị. Lỗ hổng ảnh hưởng đến VMware Avi Load Balancer 32.1.1; các phiên bản 31.1.1 đến 31.2.2; 30.1.1 đến 30.2.6; 22.1.1 đến 22.1.7.

- Khuyến nghị: Nâng cấp lên phiên bản 32.1.2, 31.2.2-2p3 hoặc 30.2.7 tùy theo nhánh đang triển khai. Lỗ hổng chưa có mã khai thác công khai.

2.10. CVE-2026-65400 – Lỗ hổng thực thi mã từ xa trong tính năng Screen Sharing của macOS

- Điểm CVSS 9.8/10, mức độ rất nghiêm trọng. Tin tặc trong cùng mạng có thể gửi gói tin được chỉnh sửa đặc biệt để vượt qua xác thực, đọc/ghi tệp tùy ý và thực thi mã với quyền root. Lỗ hổng ảnh hưởng đến macOS Tahoe trước phiên bản 26.6.1, macOS Sequoia trước phiên bản 15.7.9, macOS Sonoma trước phiên bản 14.8.9.

- Khuyến nghị: Nâng cấp macOS lên phiên bản đã được vá; tắt Screen Sharing nếu không cần thiết, chặn truy cập từ mạng không tin cậy vào cổng TCP 5900. Lỗ hổng đã có mã khai thác công khai.

2.11. Khuyến nghị đối với các cơ quan, đơn vị

- Rà soát, xác định các hệ thống, thiết bị, phần mềm đang sử dụng có khả năng bị ảnh hưởng bởi các lỗ hổng nêu trên; khẩn trương cập nhật bản vá theo hướng dẫn của nhà phát hành.

- Bảo đảm tất cả máy tính sử dụng hệ điều hành Windows, macOS, trình duyệt Google Chrome được bật chức năng cập nhật tự động; khởi động lại máy tính, trình duyệt sau khi cập nhật để bản vá có hiệu lực.

- Đối với các máy chủ, thiết bị mạng (Linux, NGINX, Cisco Secure FMC, VMware Avi Load Balancer, website sử dụng WordPress), giao cán bộ phụ trách công nghệ thông tin chủ động kiểm tra phiên bản, cập nhật bản vá và theo dõi các dấu hiệu bất thường.

- Kịp thời báo cáo bộ phận phụ trách công nghệ thông tin hoặc Công an tỉnh khi phát hiện hệ thống có dấu hiệu hoạt động bất thường hoặc nghi ngờ bị tấn công.

3. Tình hình liên quan việc giám sát hệ thống thông tin quan trọng

Công an tỉnh phối hợp Liên danh Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam và Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam giám sát, đảm bảo an ninh mạng đối với các hệ thống, thiết bị phục vụ hệ thống thông tin quan trọng dùng chung của tỉnh. Đến nay, hệ thống SOC đã vận hành, đang từng bước kết nối với các hệ thống thông tin trên địa bàn tỉnh, thực hiện chia sẻ thông tin, dữ liệu giám sát an ninh mạng với Trung tâm An ninh mạng quốc gia, góp phần nâng cao năng lực giám sát, phát hiện sớm và cảnh báo các nguy cơ, sự cố an ninh mạng; kịp thời hỗ trợ xử lý, ứng phó với các cuộc tấn công mạng, bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin trên địa bàn tỉnh.

4. Tình hình lây nhiễm mã độc tại các cơ quan, đơn vị trên địa bàn tỉnh

Trong tháng 9/2026 phát hiện **1.630** lượt kết nối tại máy tính của cán bộ công chức trong các cơ quan nhà nước tỉnh đến máy chủ chứa mã độc, phát sinh tại 28 cơ quan, đơn vị; một số đơn vị có lượt kết nối lớn như Sở Y tế (*1.097 lượt*), Sở Văn hóa, Thể thao và Du lịch (*120 lượt*), UBND xã Đức Hợp (*108 lượt*), UBND xã Bình Nguyên (*76 lượt*). Phân tích thông tin IOC cho thấy phần lớn các kết nối liên quan đến các trang web có nội dung độc hại (porn site) và các máy chủ khai thác tiền ảo trái phép (Crypto Mining); ngoài ra còn ghi nhận kết nối liên quan đến các dòng mã độc Trojan, tupym, gamarue, mạng máy tính ma (botnet) và hạ tầng có dấu hiệu liên quan đến nhóm tấn công có chủ đích (APT).

Đơn vị	Kết nối mã độc	Danh sách IP nhiễm	Loại mã độc
Sở Y tế	1097	10.181.164.44	porn site
Sở Văn hóa, Thể thao và Du lịch	120	10.181.165.118, 10.181.165.167, 10.181.165.20, 10.181.165.21,	crypto mining, porn site

		10.181.165.22, 10.181.165.24, 10.181.165.25, 10.181.165.26, 10.181.165.34, 10.181.165.42, 10.181.165.44, 10.181.165.48	
UBND Xã Đức Hợp	108	10.181.130.168, 10.181.130.22, 10.181.130.47, 10.181.130.48, 10.181.130.65	porn site
UBND Xã Bình Nguyên	76	10.181.108.11, 10.181.108.12, 10.181.108.15	crypto mining
UBND Xã Như Quỳnh	23	10.181.148.51, 10.181.148.68	Trojan, porn site
UBND Xã Quang Lịch	18	10.181.103.48	porn site
UBND Xã Vạn Xuân	17	10.181.115.12, 10.181.115.13	porn site
UBND Xã Chí Minh	16	10.181.139.29, 10.181.139.31	porn site
Thanh tra tỉnh	16	10.181.166.142, 10.181.166.149, 10.181.166.77	botnet, porn site
UBND Xã Vũ Thư	15	10.181.110.215, 10.181.110.40, 10.181.110.45, 10.181.110.98	porn site
UBND Xã Thái Ninh	13	10.181.62.10	porn site
UBND Phường Mỹ Hào	13	10.181.145.34	porn site
UBND Xã Hồng Quang	12	10.181.135.42	porn site
UBND Xã Khoái Châu	10	10.181.136.22	crypto mining
UBND Xã Tổng Trân	10	10.181.126.45, 10.181.126.70	gamarue (malware)
Sở Công Thương	10	10.181.157.17	crypto mining
UBND Phường Sơn Nam	10	10.181.117.104	porn site
UBND Xã Bắc Tiên Hưng	8	10.181.85.10	apt
UBND Xã Nam Tiên Hưng	7	10.181.91.32	tupym (malware)
UBND Xã Hưng Hà	6	10.181.93.21, 10.181.93.28	porn site
UBND Xã Tiền Hải	6	10.181.67.130	tupym (malware)
UBND Xã Đông Hưng	6	10.181.84.42	porn site
UBND Xã Mỹ Sở	5	10.181.154.37, 10.181.154.51	porn site, tupym (malware)
UBND Xã Văn Giang	2	10.181.153.26	porn site
UBND Xã Đông Tiên Hưng	2	10.181.86.47	porn site

UBND Xã Phạm Ngũ Lão	2	10.181.133.34	porn site
UBND Xã Phú Đức	1	10.181.82.13	crypto mining
UBND Xã Tây Thụy Anh	1	10.181.66.37	porn site
Tổng cộng	1.630		

II. NHẬN XÉT

1. Trong tháng 9/2026, tình hình an ninh mạng tiếp tục diễn biến phức tạp. Các nhóm tin tặc có chủ đích (APT) như Mustang Panda và các nhóm sử dụng mã độc VShell vẫn duy trì hoạt động, nhắm vào hệ thống thông tin của cơ quan nhà nước, doanh nghiệp; sử dụng các kỹ thuật lợi dụng phần mềm hợp pháp, tệp tin giả mạo thư mời, tài liệu, thực thi mã độc trực tiếp trên bộ nhớ để né tránh phát hiện, đồng thời xuất hiện xu hướng sử dụng trí tuệ nhân tạo để tự động hóa chuỗi tấn công mạng.

2. Trong kỳ, 10 lỗ hổng bảo mật nghiêm trọng được công bố (06 lỗ hổng mức độ rất nghiêm trọng, 08 lỗ hổng đã có mã khai thác công khai), ảnh hưởng đến nhiều sản phẩm phổ biến đang được sử dụng tại các cơ quan, đơn vị như hệ điều hành Windows, Linux, macOS, trình duyệt Google Chrome, máy chủ web NGINX, WordPress và thiết bị tường lửa. Nguy cơ bị khai thác là rất cao nếu các cơ quan, đơn vị không kịp thời cập nhật bản vá.

3. Kết quả giám sát cho thấy trong tháng 9/2026 có 1.630 lượt kết nối từ máy tính tại 28 cơ quan, đơn vị đến máy chủ chứa mã độc, trong đó riêng Sở Y tế chiếm 1.097 lượt (khoảng 67,3% tổng số lượt kết nối). Các kết nối chủ yếu liên quan đến trang web có nội dung độc hại và khai thác tiền ảo trái phép, phản ánh việc quản lý, sử dụng thiết bị đầu cuối và truy cập Internet tại một số đơn vị chưa chặt chẽ, cần tiếp tục được tăng cường.

4. Với xu hướng các chiến dịch tấn công mạng ngày càng tinh vi, có sự hỗ trợ của trí tuệ nhân tạo, nguy cơ bị khai thác lỗ hổng, lây nhiễm mã độc, đánh cắp dữ liệu hoặc chiếm quyền tài khoản đối với các cơ quan nhà nước vẫn ở mức cao nếu không triển khai đồng bộ các biện pháp bảo đảm an ninh mạng.

III. KIẾN NGHỊ, ĐỀ XUẤT

Nhằm chủ động phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ gây mất an ninh mạng, Công an tỉnh đề nghị các sở, ban, ngành, đơn vị, địa phương thực hiện tốt một số nội dung sau:

1. Đề nghị các sở, ban, ngành; UBND các xã, phường tiếp tục quán triệt và thực hiện nghiêm các quy định về bảo đảm an ninh mạng; tăng cường tuyên truyền, phổ biến cho cán bộ, công chức, viên chức về các phương thức, thủ đoạn tấn công mạng mới, đặc biệt là thủ đoạn phát tán mã độc qua tệp tin giả mạo thư mời, tài liệu (tệp shortcut .lnk, tệp nén), lợi dụng phần mềm hợp pháp và các website không rõ nguồn gốc.

2. Chỉ đạo bộ phận phụ trách công nghệ thông tin thường xuyên kiểm tra, cập nhật hệ điều hành, trình duyệt và các phần mềm, thiết bị đang sử dụng lên phiên bản mới nhất, đặc biệt đối với các lỗ hổng đã nêu tại Mục I.2 của báo cáo; bảo đảm tất cả máy tính được cài đặt phần mềm phòng, chống mã độc và cập nhật đầy đủ các bản vá bảo mật.

3. Tăng cường kiểm tra, giám sát các máy chủ, máy trạm; chủ động rà soát theo các dấu hiệu nhận biết (IOC) của mã độc Mustang Panda, VShell và các chiến dịch tấn công nêu trên; tổ chức xử lý triệt để các thiết bị có dấu hiệu lây nhiễm mã độc, đồng thời thực hiện đổi mật khẩu đối với các tài khoản có nguy cơ bị lộ lọt thông tin xác thực.

4. Đề nghị các đơn vị có máy tính phát sinh kết nối đến máy chủ chứa mã độc khẩn trương kiểm tra, xác minh nguyên nhân, thực hiện quét mã độc trên toàn bộ máy tính thuộc phạm vi quản lý; báo cáo kết quả xử lý về Công an tỉnh để theo dõi, tổng hợp.

5. Đề nghị các thành viên Đội ứng cứu sự cố an ninh mạng tỉnh tại các sở, ban, ngành, UBND các xã, phường chủ động phối hợp với Công an tỉnh trong công tác rà soát, xử lý mã độc, ứng cứu sự cố; kịp thời tiếp nhận và triển khai các cảnh báo an ninh mạng đến cán bộ, công chức, viên chức thuộc đơn vị mình.

6. Tiếp tục duy trì cơ chế phối hợp giữa Công an tỉnh, đơn vị vận hành Trung tâm giám sát an ninh mạng tỉnh và các cơ quan, đơn vị trong việc chia sẻ thông tin, giám sát, cảnh báo sớm và xử lý các nguy cơ, sự cố; kịp thời báo cáo Công an tỉnh khi phát hiện dấu hiệu tấn công mạng hoặc mất an ninh mạng để phối hợp xử lý.

7. Đề nghị UBND tỉnh tiếp tục quan tâm bố trí nguồn lực phục vụ công tác bảo đảm an ninh mạng; chỉ đạo các cơ quan, đơn vị triển khai đồng bộ các giải pháp kỹ thuật, nâng cao năng lực giám sát, phát hiện, cảnh báo sớm và ứng cứu sự cố an ninh mạng, góp phần bảo đảm hoạt động ổn định, an toàn của các hệ thống thông tin phục vụ chuyển đổi số trên địa bàn tỉnh.

Trên đây là báo cáo về tình hình An ninh mạng trong các cơ quan nhà nước tỉnh Hưng Yên tháng 9/2026. Công an tỉnh báo cáo UBND tỉnh, gửi các Sở, Ban, Ngành, UBND xã, phường biết, chủ động khắc phục và phối hợp xử lý./. *AN*

Nơi nhận:

- UBND tỉnh (để báo cáo);
- Đ/c Giám đốc Công an tỉnh (để báo cáo);
- UBND các xã, phường (để phối hợp);
- Các Sở, ban, ngành tỉnh (để phối hợp);
- Lưu: VT, ANM(Đ2).



Đại tá Nguyễn Trường Lâm